

The diagram illustrates the architecture of the Analysis/Target Machine, divided into User Mode and Kernel Mode.

**User Mode:**

- Analysis/Target Machine:** This block contains:
  - Command Line Interpreter (108):** Receives input from the **Collection Driver (100)** via the **Communication/Driver Interface (104)**.
  - Communication/Driver Interface (106):** Facilitates communication between the **Collection Driver (100)** and the **Command Line Interpreter (108)**.
  - Symbol Manager (120):** Manages symbols and interacts with the **Symbol File Library (122)**.
  - Framework (110):** The core component that interacts with the **Command Plug-in (112)** and the **OS Kernel (114)**.
  - Symbol File Library (122):** Stores symbol information.
  - Command Plug-in (112):** Interacts with the **Framework (110)** and the **OS Kernel (114)**.
  - Command Plug-in (118):** Another instance of a command plug-in.

**Kernel Mode:**

- Collection Driver (100):** Receives input from the **OS Kernel (114)** and the **Drivers (116)**.
- OS Kernel (114):** The operating system kernel that manages the **Collection Driver (100)** and the **Drivers (116)**.
- Drivers (116):** Hardware drivers that interface with the **OS Kernel (114)**.

Arrows indicate the flow of data and control between these components.

Figure 1, Local

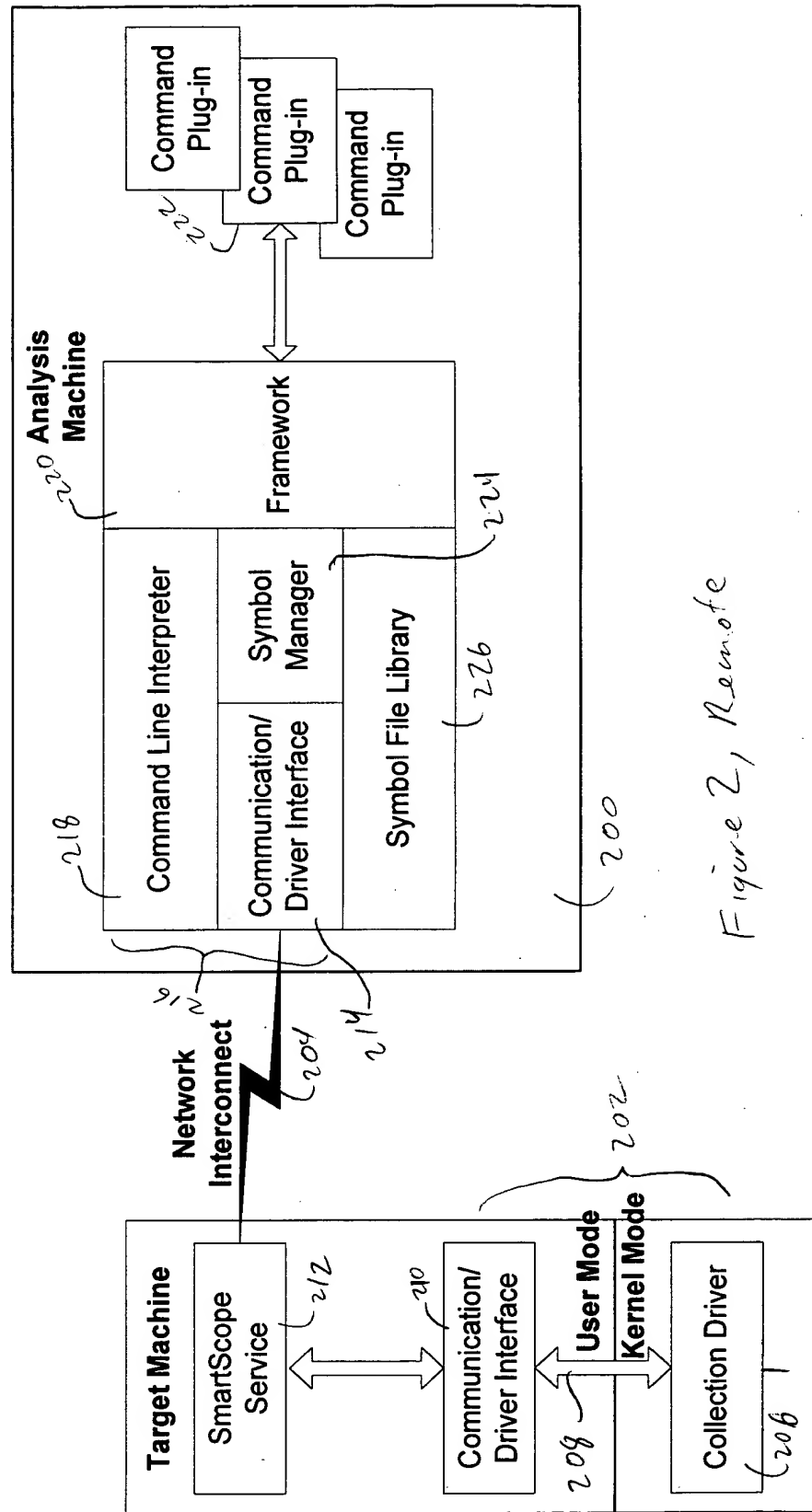
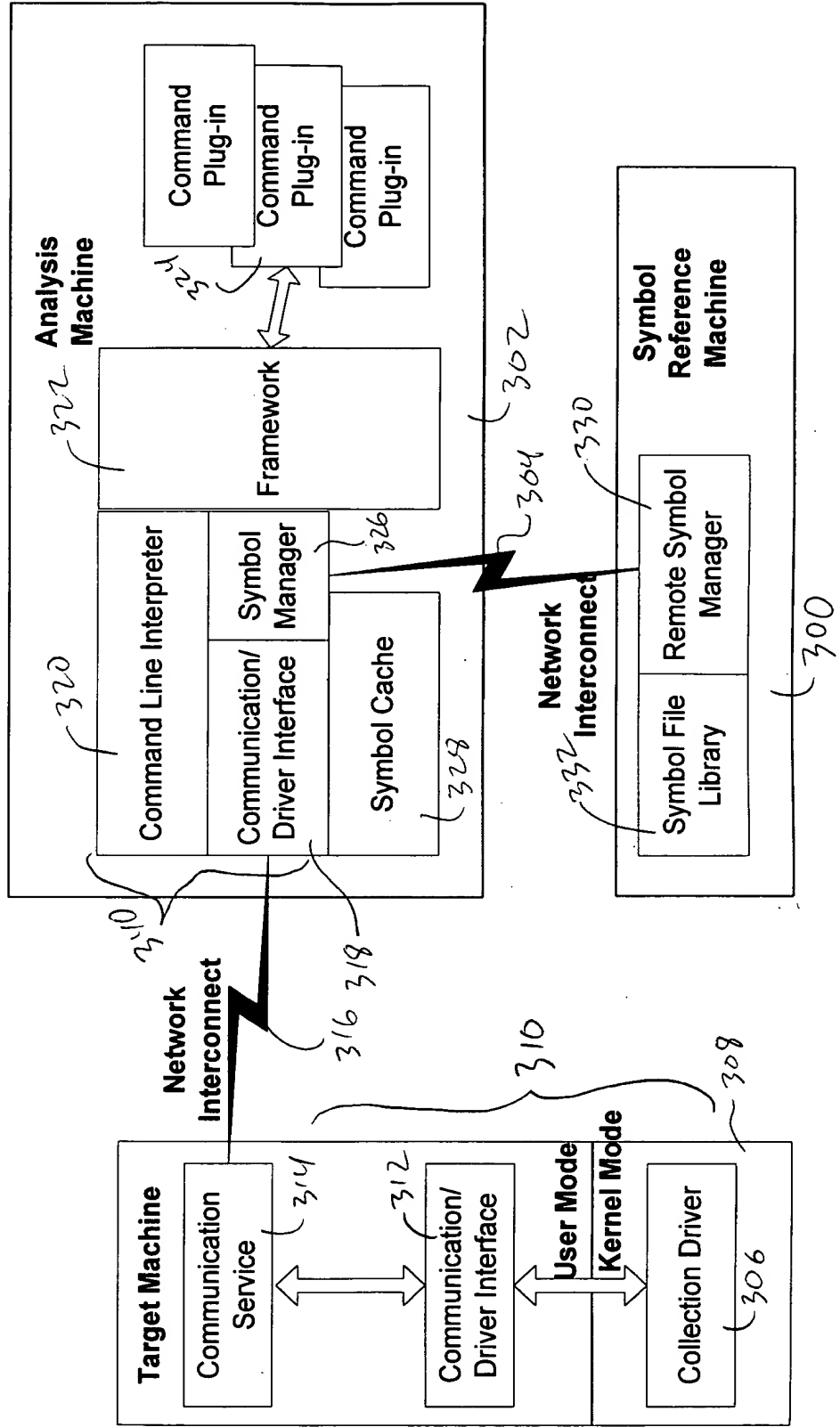


Figure 2, Remote

Figure 3, Central Symbol Library



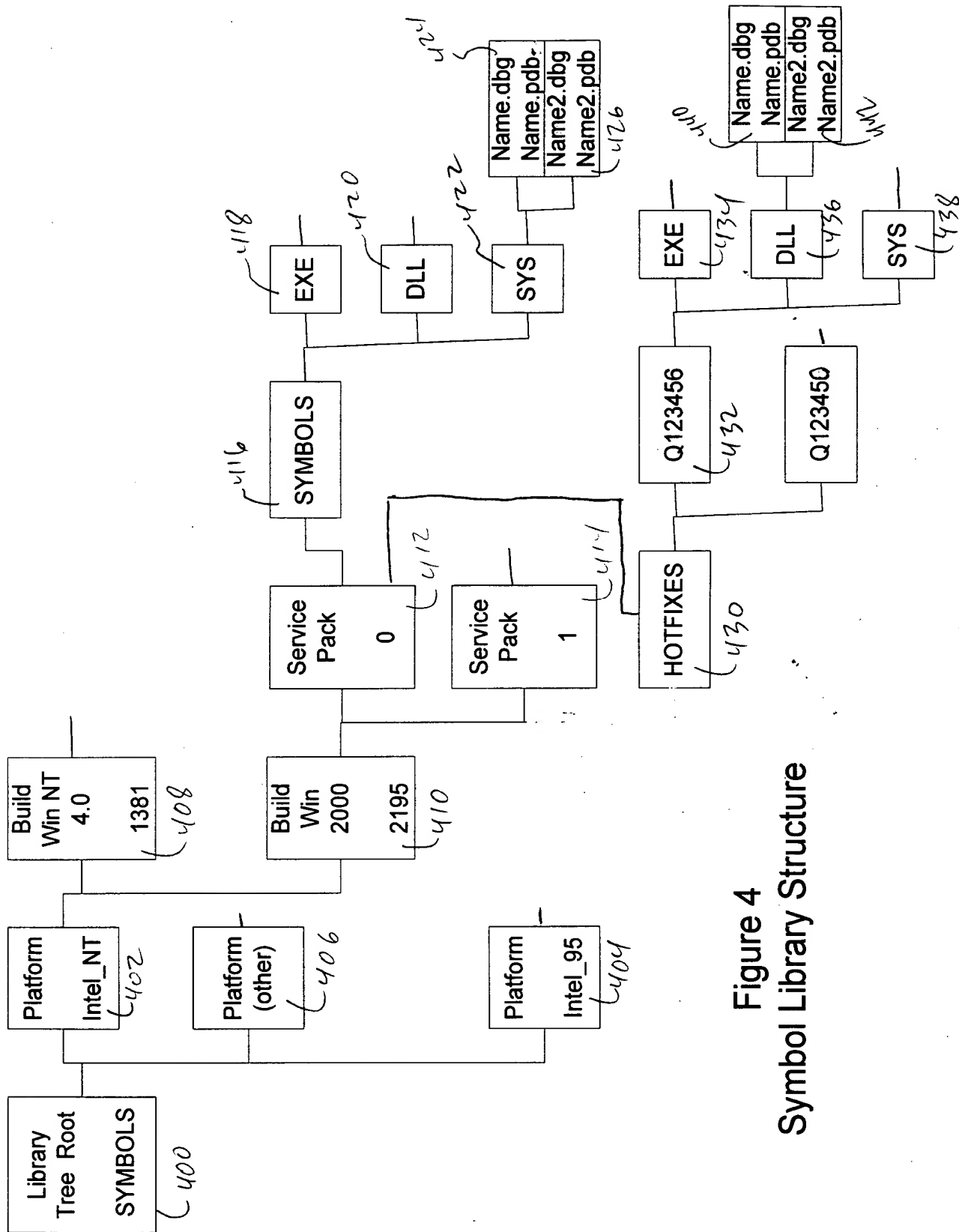


Figure 4  
Symbol Library Structure

09706075 "110300

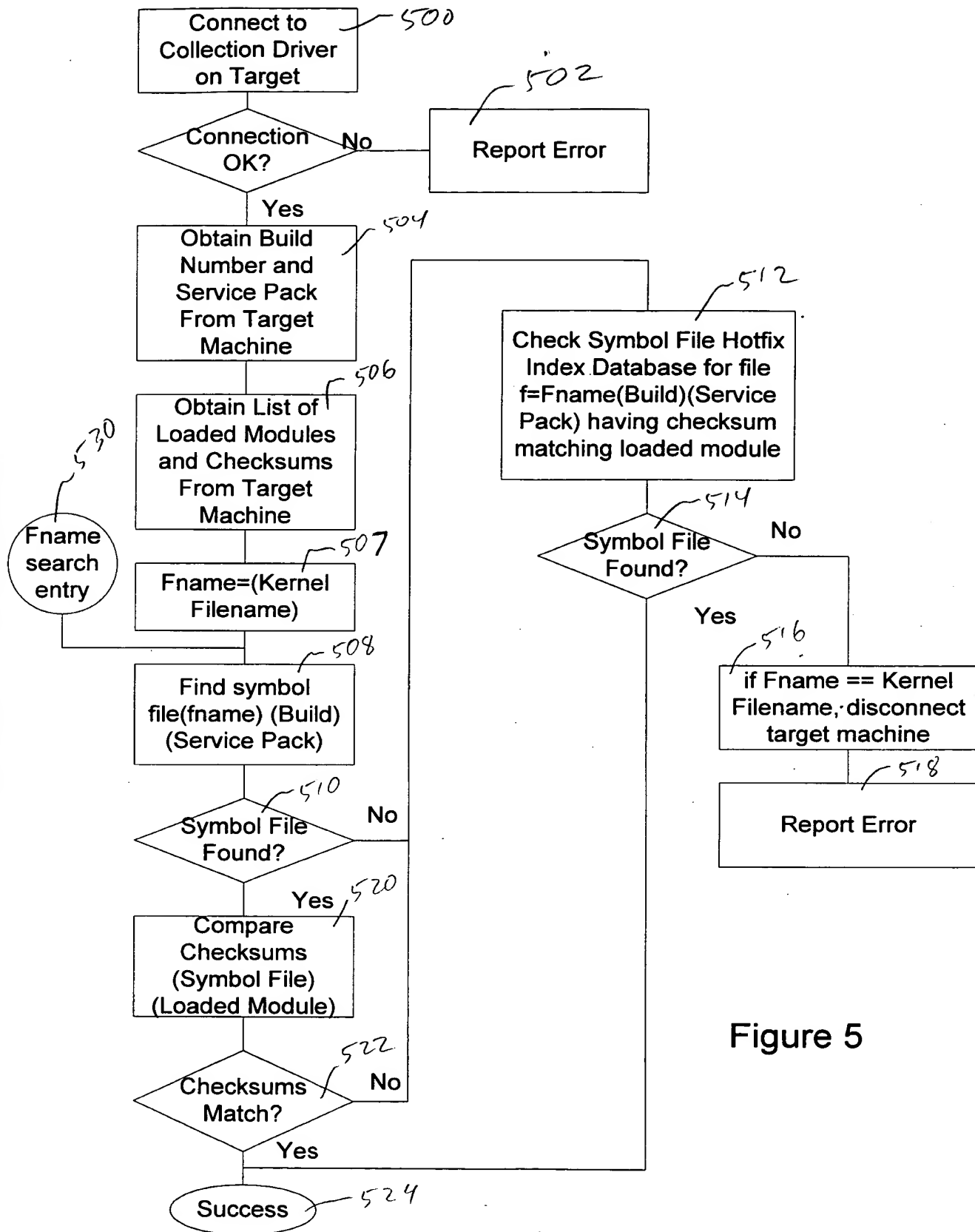


Figure 5

09706076 "110300

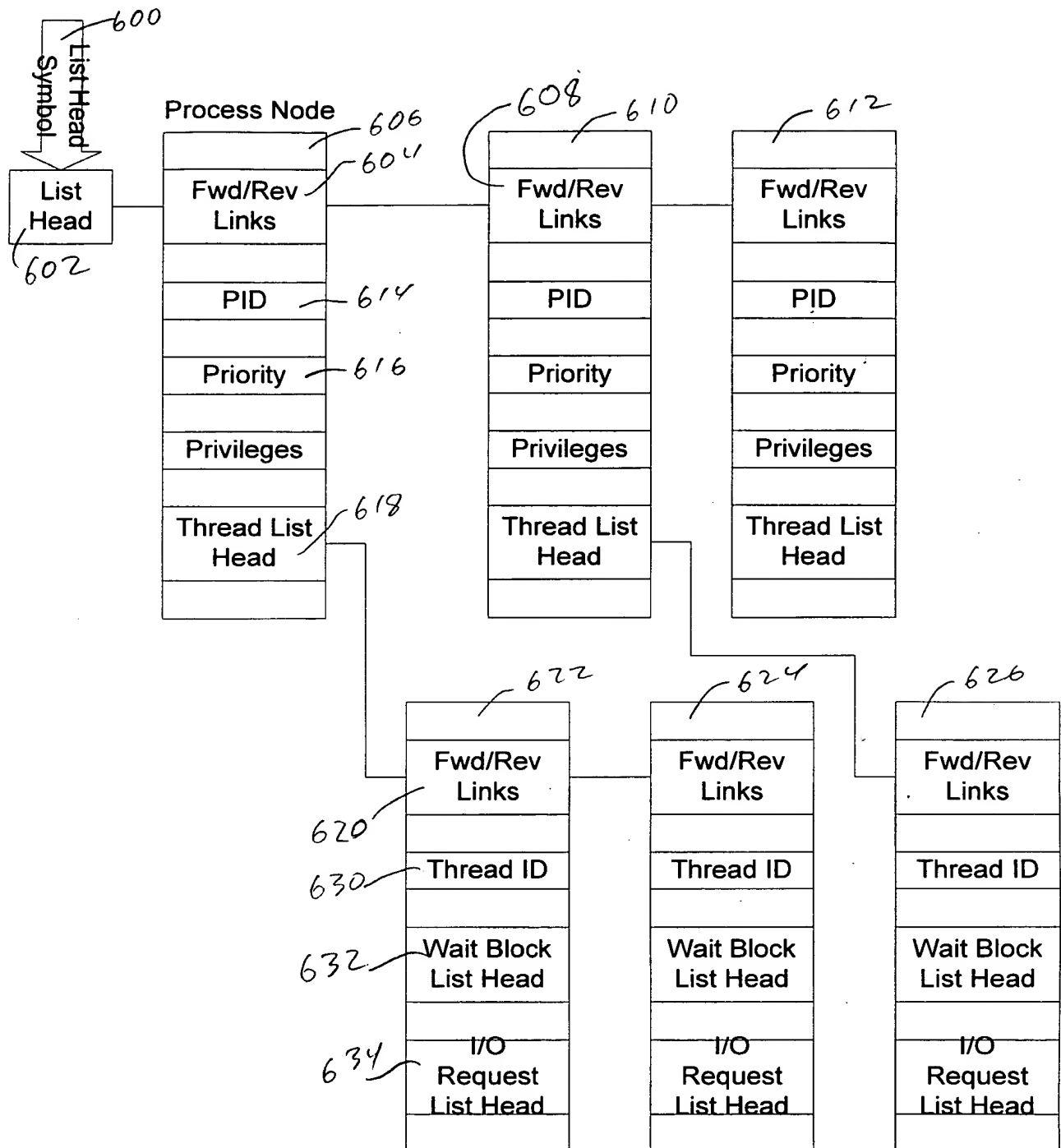
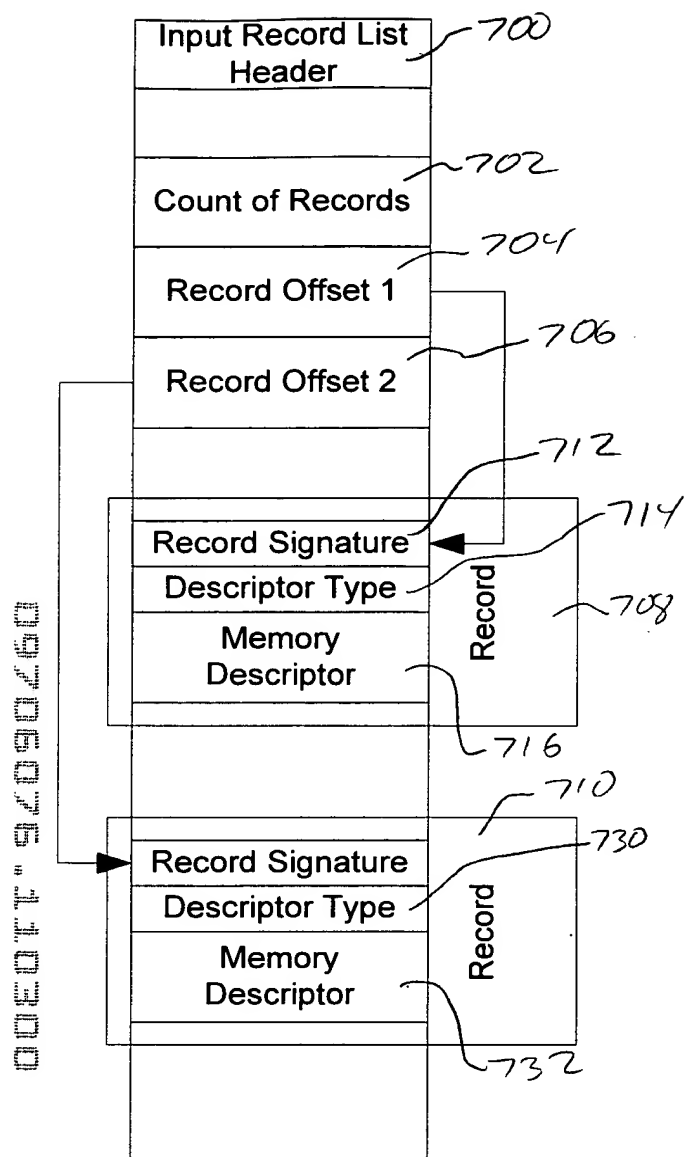
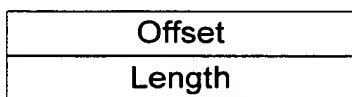


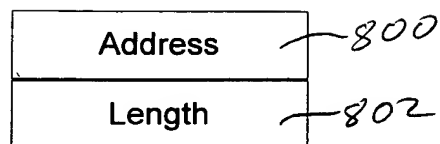
Figure 6  
KNOWN ART  
Windows NT/2000 Process List Structure



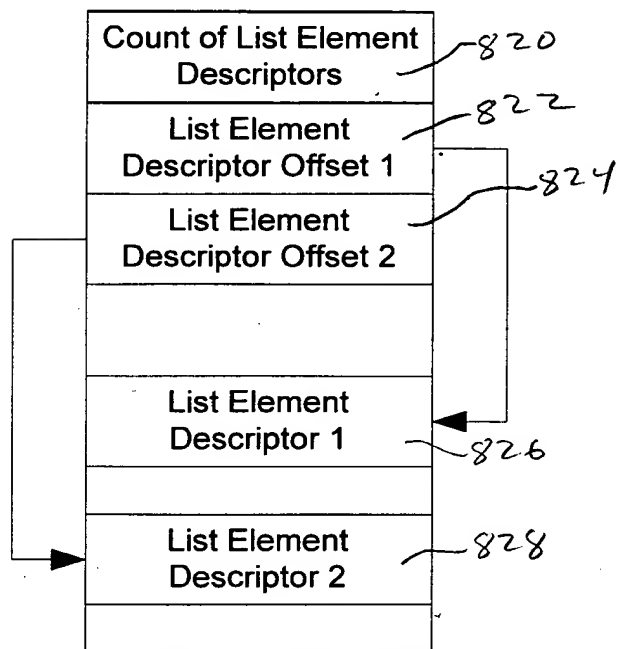
**Figure 7**  
Input Record List Structure



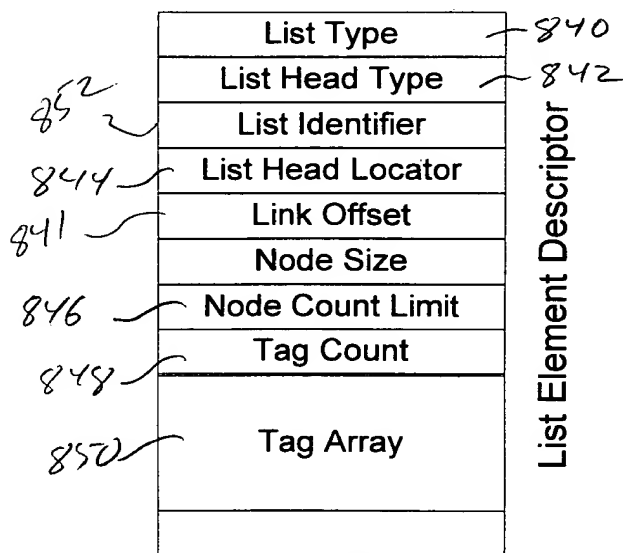
**Figure 8D**  
Tag



**Figure 8A**  
Scalar Memory Descriptor



**Figure 8B**  
List Memory Descriptor



**Figure 8C**

09706076-110300

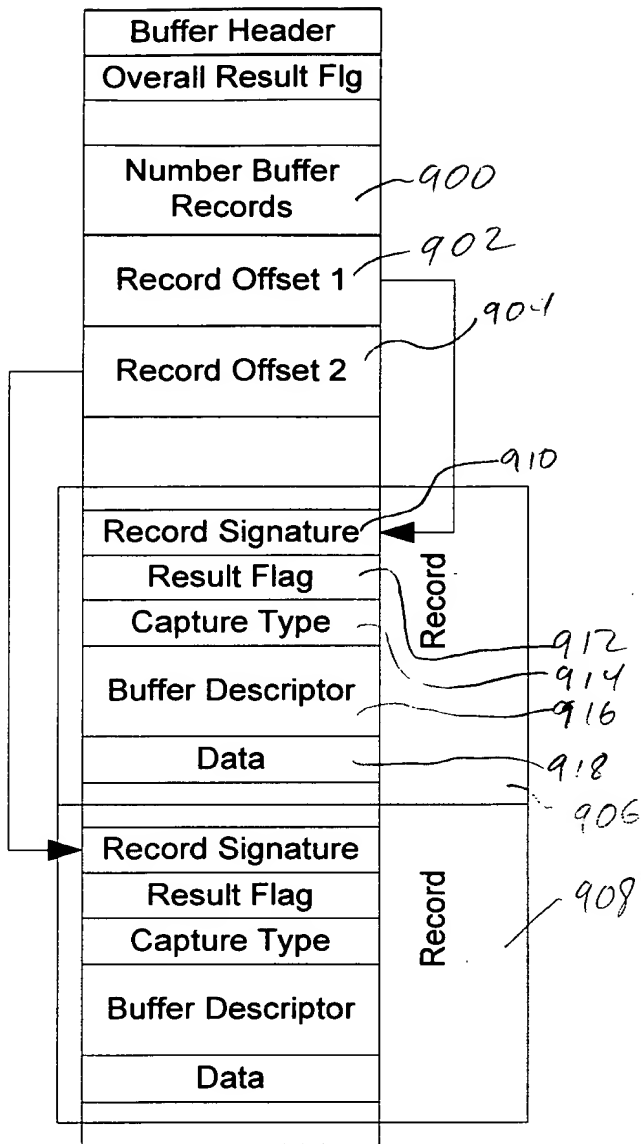


Figure 9  
Capture Buffer Structure

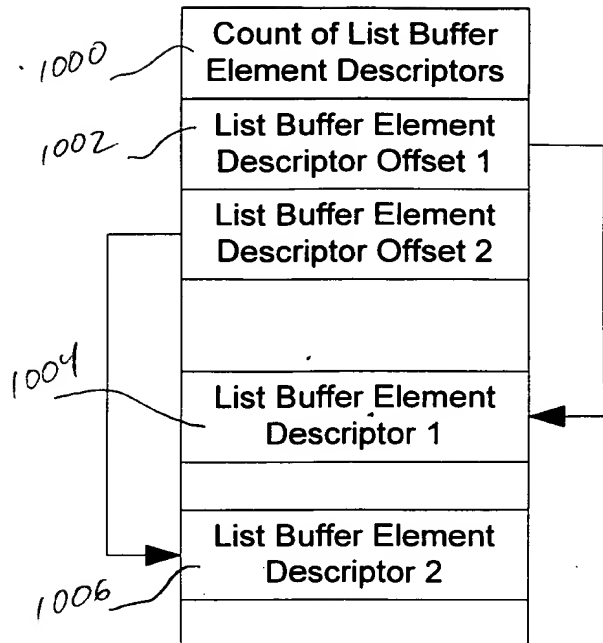


Figure 10  
List Buffer Descriptor

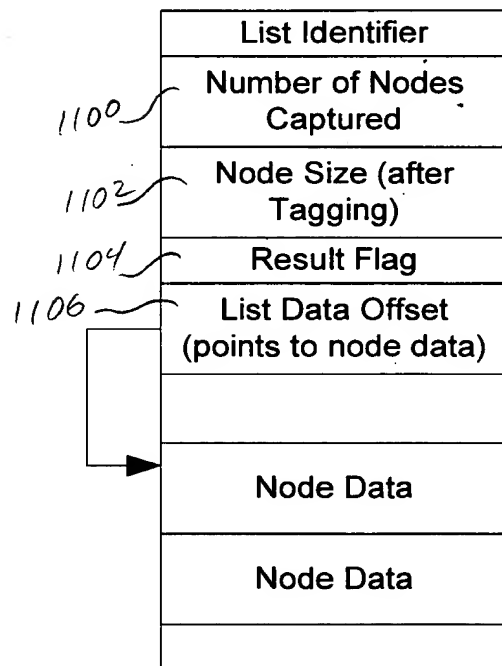


Figure 11  
List Buffer Element Descriptor